



AF
JFW

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Inventor(s): Douglas N. Knisely
Robert Jerrold Marks
Semyon B. Mizikovsky

Case: 7-4-28

Serial No.: 09/662580 Group Art Unit: 2135

Filing Date: September 15, 2000

Examiner: P. W. Klimach

Title: Method For Distributing Encryption Keys For An Overlay Data Network

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Enclosed in triplicate is an Appeal Brief in the above-identified patent application.

Please charge the amount of \$500 covering payment of the fee for the Appeal Brief, to **Lucent Technologies Inc. Deposit Account 12-2325**. Triplicate copies of this letter are enclosed.

In the event of non-payment or improper payment of a required fee, the Assistant Commissioner is authorized to charge or to credit **Deposit Account No. 12-2325** as required to correct the error.

Respectfully,

Martin I. Finston
Attorney for the Applicant
Reg. No. 31,613
(973)-386-3147

Date: July 7, 2006

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Mail Stop **APPEAL BRIEF-PATENTS**, Director of the US Patent and Trademark Office, PO Box 1450, Alexandria, VA 22313-1450, on
July 7, 2006.

Margaret Cardoso



PATENT

IN THE U.S. PATENT AND TRADEMARK OFFICE

Appellant: D.N. Knisely
R.J. Marks
S. Mizikovsky

Application No.: 09/662580

Art Unit: 2135

Filed: September 15, 2000

Examiner: Paula W. Klimach

For: METHOD FOR DISTRIBUTING ENCRYPTION KEYS FOR AN
OVERLAY DATA NETWORK

Atty. Dkt. No.: D.N. KNISELY 7-4-28

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22313
Mail Stop Appeal Brief – Patent

July 7, 2006

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

Appellant submits herewith their Brief on Appeal as required by 37 C.F.R. § 41.37.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Director of the US Patent and Trademark Office, PO Box 1450, Alexandria, VA 22313-1450, on July 7, 2006. Margaret Cardoso
Margaret Cardoso

07/11/2006 MBELETE1 00000004 122325 09662580

01 FC:1402 500.00 DA

TABLE OF CONTENTS

	<u>Page</u>
BRIEF ON BEHALF OF APPELLANT	3
I. REAL PARTY IN INTEREST	3
II. RELATED APPEALS AND INTERFERENCES.....	3
III. STATUS OF CLAIMS	3
IV. STATUS OF AMENDMENTS	3
V. SUMMARY OF CLAIMED SUBJECT MATTER	3
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	5
VII. ARGUMENTS.....	6
A. Claims 29-30 are not unpatentable over the combination of Marvit in view of Burrows and further in view of Stallings.....	6
1. Claim 29.....	6
2. Claim 30.....	10
VIII. EVIDENCE AND RELATED APPEALS APPENDICES:.....	12
IX. CONCLUSION.....	13
X. CLAIMS APPENDIX.....	14

BRIEF ON BEHALF OF APPELLANT

In support of the Notice of Appeal filed on April 17, 2006, appealing the Examiner's final rejection mailed on December 22, 2005 of each of pending claims 29-30 of the present application which appear in the attached claims appendix (Section X), Appellant hereby provides the following remarks.

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is Lucent Technologies Inc.

II. RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

III. STATUS OF CLAIMS

Claims 29-30 are pending in the application, with both claims being independent.

Claims 29-30 remain finally rejected under 35 U.S.C. § 103 (a) as being unpatentable over Marvit (U.S. Patent No. 6,625,734) in view of the article by Burrows et al. (hereinafter "Burrows") and further in view of the book by Stallings, Cryptography and Network Security (hereinafter, "Stallings").

Claims 29-30 are being appealed.

IV. STATUS OF AMENDMENTS

Appellant filed an Amendment on October 20, 2005 to cancel claims 1-28 and to amend claims 29-30. The Examiner entered this Amendment. Accordingly, the claims in Appendix X reflect the status of the current claims with the October 20, 2005 amendment.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed invention is directed to a method for a mobile station to authenticate itself to a new network B, taking advantage of the circumstances that: (i) the mobile station is already authenticated to an old network A, and (ii) there exists a secure channel for communication between networks A and B.

In Figure 3 of the application, for example, the mobile station is identified by reference numeral 62. Mobile station 62 has already been authenticated to network 50, which thus has the role of “old network A”. Network 60 in Figure 3 is the “new network B” to which the mobile station wishes to be authenticated.

The method as recited in the claims involves the mobile station identifying itself in a request to network B. Network B forwards the mobile’s ID (such as the IMSI) to Network A together with an authentication key (such as SSD). Network A forwards the authentication key to the mobile station under the protection of an encryption key that has been established between Network A and the mobile station. The mobile station generates an authentication signature and sends it to Network A for forwarding to Network B. The authentication signature is generated from the mobile ID and the authentication key. For example, the authentication signature might be $(\text{IMSI})_{\text{SSD}}$, i.e., the IMSI encrypted by SSD. When Network B receives the authentication signature, it decides whether to accept it. If the authentication signature is accepted, the mobile station can enter into communication with Network B.

Figure 4 of the application illustrates a protocol which includes examples of the steps described above. The protocol of Figure 4 applies to a particular network configuration which is illustrated in Figure 3. A more detailed examination of Figure 3 will show that network 60 is an HDR network which is in communication with a packet data service network (PDSN) identified by the reference numeral 116. Moreover, wireless terminal 62 is shown connected to an application terminal 100. (Specification, page 3, lines 19-29.)

For purposes of data communication, application terminal 100 communicates wirelessly via mobile terminal 62. Data communications are transported to ultimate destinations by packet data service network (PDSN) 116. Wireless communication with PDSN 116 is supported by HDR network 60. (Specification, page 3, lines 22-29.)

The correspondences between the above-described steps and steps of the illustrated protocol are listed below:

Step as described above	Protocol step (Figure 4)	Cite to Specification
Network B forwards the mobile's ID to Network A together with an authentication key.	(h) The HDR RAN (of network 60) sends a message to network 50. The message contains IMSI (the mobile ID) and HDR_SSD (the authentication key).	page 4, lines 17-22.
Network A forwards the authentication key to the mobile station under the protection of an encryption key that has been established between Network A and the mobile station.	(i) Network 50 encrypts the message using the key K_c and sends it to mobile station 62.	page 4, lines 23-24.
The mobile station generates an authentication signature and sends it to Network A for forwarding to Network B.	(j) Mobile station 62 decrypts the message and sends it to application terminal 100 to which the mobile station is connected . (k) Application terminal 100 calculates a digital signature of IMSI using HDR_SSD as the key, and returns the result to the mobile station. (l) Mobile station 62 sends a message to network 50 for forwarding to network 60. The message contains the digital signature of IMSI computed in step (k).	page 4, lines 25-32.
Network B decides whether to accept the authentication key.	(n) The HDR RAN validates the digital signature of IMSI.	page 4, line 34.
Network B permits communication with the mobile station.	(o)-(s) The HDR RAN establishes a PPP session between application terminal 100 and packet data service network (PDSN) 116.	page 5, lines 1-8.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant seeks the Board's review of the rejection of claims 29-30 under 35 U.S.C. § 103(a) as being unpatentable over Marvit (U.S. Patent No. 6,625,734) in view of the article by Burrows et al. (hereinafter "Burrows") and further in view of the book by Stallings, Cryptography and Network Security (hereinafter, "Stallings").

VII. ARGUMENTS

A. Claims 29-30 are not unpatentable over the combination of Marvit in view of Burrows and further in view of Stallings.

Claims 29 and 30 relate to the same authentication process, but from different points of view. That is, claim 29 describes actions which are to be performed by the mobile station, whereas claim 30 describes actions which are to be performed by the “old network A” to which the mobile station has already been authenticated. Although they relate to the same authentication process, claims 29 and 30 relate to different aspects of that process. Therefore, the claims stand and fall separately.

1. Claim 29

The combination of Marvit, Burrows, and Stallings does not teach or suggest any scenario in which a mobile station seeking to authenticate itself to a network B obtains an authentication key from a further network A and uses network A, as a trusted agent, to forward an authentication message to network B.

More specifically, the cited combination of references fails to teach or suggest a scenario in which: A mobile station sends a mobile station identifier to network B, the mobile station securely obtains from network A an authentication key SSD which is a secret shared among network A, network B, and the mobile station, the mobile station sends the identifier encrypted with SSD to network A in an authentication message for forwarding to network B, and the mobile station enters into communications with network B if network B accepts the authentication message.

Further, as will be discussed below, the Examiner has not established the requisite motivation to combine Marvit and Burrows.

a. Marvit fails to suggest an authentication procedure, and in particular fails to suggest having a trusted agent provide the authentication key and forward the resulting authentication message.

To facilitate comparison between the present invention and the cited art, a uniform terminology will be adopted. In accordance therewith, two entities, labeled M and B, are seeking to establish communication with each other, with the help of a trusted agent A. The labels “M”, “A”, and “B” are chosen to correspond with the terminology used in the present

claims, so that the mobile station is identified with M, Network B is identified with B, and Network A is identified with the trusted agent A.

In Marvit, A provides an encryption key to M and a decryption key to B (or *vice versa*). M uses the encryption key to send an encrypted message to B. B uses the decryption key to decrypt the message.

What is described here is purely a method of distributing a pair of keys to respective parties. The particular identity of M is of no concern whatsoever. For that reason among others, there lacks any suggestion to perform an authentication procedure. Much less, then, is there any suggestion to invoke the aid of A in performing an authentication procedure.

By contrast, the the inventive process may be summarized in pertinent part by the following steps:

- (i) M sends its ID directly to B.
- (ii) A sends SSD to M. SSD is known to B.
- (iii) M encrypts the ID with SSD to generate an authentication signature.
- (iv) M then uses A to forward the authentication signature to B.

All four of the above steps relate directly to the authentication of M to B, and (i), (iii), and (iv) rely explicitly on knowledge of "ID", i.e., of the identity of M.

The Examiner has argued that Marvit suggests step (ii), while completely ignoring steps (i), (iii), and (iv) and the essential manner in which they cooperate with step (ii).

Moreover, the analogy that the Examiner attempts to make between Marvit and the above step (ii) is based on a misunderstanding. Marvit has the trusted agent distribute a key for encryption or a key for decryption to each of the parties. The purpose of those keys is, respectively, to lock and to unlock messages. Typically, only one party will be in possession of each key.

By contrast, it is an essential aspect of SSD that it be a shared secret among the parties, specifically so that it can be used to authenticate one party to another. Because SSD is used for the specific purpose of generating an authentication signature, and not for the purpose of locking or unlocking messages, there is no valid analogy between SSD and the keys discussed by Marvit.

Thus, Marvit completely fails to suggest any use of A to support an authentication process.

- b. Burrows likewise fails to suggest an authentication procedure, or in particular having a trusted agent provide the authentication key and forward the resulting authentication message.**

In Burrows at page 18, A is a source of a key K for communication between M and B. A distributes the key K directly to M under the protection of a further key K_{MA} . A distributes the key K indirectly to B; that is, A encrypts K with the further key K_{BA} , encrypts the result with the key K_{MA} , and sends the resulting message to M. M decrypts the message with respect to K_{MA} and forwards the result to B.

In Burrows at page 25, M is the source of the key K for communication between M and B. The trusted agent A is used to forward K from M to B. The key K goes from M to A under the protection of K_{MA} , and then it goes from A to B under the protection of K_{BA} .

In both of the above-cited passages from Burrows, A is the trusted agent, since it alone is in possession of both a shared key with M and a shared key with B. However, as in Marvit, A is used solely for purposes of key distribution, and not for the purpose of authenticating one party to another. In neither passage of Burrows is there any suggestion to invoke the particular identity of either M or B for any purpose. On the contrary, it is assumed that M and B are already known to A, since A already shares keys with those parties. For that reason among others, there lacks any suggestion to perform an authentication procedure. Much less, then, is there any suggestion to invoke the aid of A in performing an authentication procedure.

- c. There is no motivation to combine Marvit with Burrows.**

There is no motivation to combine Marvit with Burrows at page 18 or Burrows at page 25, because Marvit teaches in a direction contrary to the cited sections of Burrows. That is, Burrows at both page 18 and page 25 teaches a key distribution method whose outcome is that M and B both possess the same key for communicating with each other. If this were the case, there would be no need for one party to obtain an encryption key, and the other party to obtain a decryption key, on a message-by-message basis as taught by Marvit.

Furthermore, Burrows at page 18 teaches that the trusted agent A communicates directly only with M. This contradicts Marvit, where the trusted agent (i.e., the key repository) communicates directly with both parties.

Still further, Burrows at page 25 teaches that M is the source of the key, and the trusted agent A merely forwards the key to B. This contradicts Marvit, where the trusted agent is the source of the keys.

d. Stallings teaches away from the claimed authentication message and the claimed manner of forwarding it.

The Examiner has admitted that Marvit and Burrow do not disclose sending the ID of the device that is seeking authentication (i.e., the mobile station). (Office Action mailed December 22, 2005, page 5, second full paragraph.) To remedy this deficiency, the Examiner has cited Stallings as disclosing an Initiator and a Responder. Initiator sends its ID to Responder. Responder authenticates Initiator, and then communication begins between the respective parties.

What Stallings actually discloses is a key distribution scenario, which includes certain authentication steps. There is a trusted agent, referred to as the Key Distribution Center (KDC), but which will here be referred to as “Agent”. The object is to distribute a session key to the parties. Initiator provides its ID to Agent, and obtains the session key from Agent. Together with the session key, Initiator obtains from Agent a message which Initiator is to forward to Responder.

To prevent Initiator from tampering with the message before forwarding it, Agent encrypts the message with the key that Agent shares only with Responder.

The forwarded message contains two components: the session key, and Initiator’s ID.

After Responder receives and decrypts the forwarded message, Responder executes a nonce handshake with Initiator, and then the communication session can begin.

Arguendo, the forwarded message could be deemed an authentication message, because it contains Initiator’s ID and is encrypted using a shared secret, namely, the master key that KDC shares solely with Responder.

As an authentication message, however, the forwarded message is distinctly different from the authentication message of Applicants’ claim 29. That is, the claimed authentication message is generated by using SSD for encryption, where SSD is “known only to network A, to the mobile station, and to a further network B”. That is, SSD is known to the trusted agent and to both of the parties that are to be placed in communication with each other. By contrast, the forwarded message in Stallings is encrypted using the master key between Agent

and Responder. Initiator is explicitly excluded from knowing that master key. Thus, the Stallings master key is known to only two of the three participating entities.

Moreover, Stallings expressly teaches away from the claimed procedure at least in regard to the generation and transmission of the authentication message. In Stallings, Agent generates the authentication message, and uses Initiator to forward the authentication message to Responder. By contrast, the procedure of Applicants claim 29 does the opposite: The mobile station (comparable to “Initiator”) generates the authentication message, and uses network A (comparable to “Agent”) to forward the authentication message to network B (comparable to “Responder”).

Thus, insofar as Stallings teaches an authentication method, it is incompatible with and antithetical to Applicants’ claimed method.

e. Combining Marvit or Burrows with Stallings, even if possible, would not lead to the claimed invention.

As explained above, Marvit and Burrows deal solely with key distribution, and not with authentication. As also explained above, Stallings, insofar as it describes an authentication method, teaches away from the claimed method of authentication. Because Marvit and Burrows are entirely unconcerned with any matter touching upon authentication, neither of those references provides any motivation to change the basic thrust of Stallings which, as explained above, leads away from the claimed invention.

f. Conclusion

On the grounds laid out above, it is respectfully submitted that claim 29 of the present application is patentable over the combination of Marvit, Burrows, and Stallings under the standard of 35 USC §103(a).

2. Claim 30

The combination of Marvit, Burrows, and Stallings does not teach or suggest any scenario in which the network A, acting as a trusted agent: receives from network B an identifier of the mobile station and an authentication key SSD which it then provides to the mobile station, and receives from the mobile station an authentication message which comprises the identifier encrypted with SSD which it then forwards to network B.

- a. **Marvit and Burrows fail to suggest an authentication procedure, or in particular having a trusted agent provide the authentication key and forward the resulting authentication message.**

As argued above in regard to claim 29, Marvit and Burrows are directed solely to key distribution schemes and are unconcerned with matters touching upon authentication.

- b. **Stallings teaches away from the claimed authentication message and the claimed manner of forwarding it.**

The Examiner has admitted that Marvit and Burrow do not disclose sending the ID of the device that is seeking authentication (i.e., the mobile station). (Office Action mailed December 22, 2005, page 5, second full paragraph.) To remedy this deficiency, the Examiner has cited Stallings as disclosing an Initiator and a Responder. Initiator sends its ID to Responder. Responder authenticates Initiator, and then communication begins between the respective parties.

As argued above in regard to claim 29, Stallings, to the extent it discloses an authentication method, teaches something distinctly different from the claimed method.

In the specific context of Applicants' claim 30, network A (acting as the trusted agent) must receive SSD and the mobile station ID from network B "as a result of a request sent from the mobile station to network B, said request including said identifier".

Thus, the agent receives the mobile ID from network B in response to information previously sent by the mobile station to network B. This stands in direct contrast to Stallings, in which Initiator (comparable to the mobile station of claim 30) identifies itself to the Agent (comparable to Network A of claim 30), and the Agent then forwards the Initiator's ID to Responder (comparable to Network B of claim 30).

Moreover, Applicants' claim 30 requires that after network A receives the SSD from network B, it must provide SSD to the mobile station. Therefore, as argued above in regard to claim 29, the present invention differs from Stallings at least in that all three parties must share the knowledge of SSD.

Furthermore, Applicants' claim 30 requires that network A must receive the authentication message from the mobile station and forward it to network B. As argued above in regard to claim 29, Stallings teaches directly away from this feature.

Thus, insofar as Stallings teaches an authentication method, it is incompatible with and antithetical to Applicants' claimed method.

c. Combining Marvit or Burrows with Stallings, even if possible, would not lead to the claimed invention.

As explained above in regard to claim 29, Marvit and Burrows deal solely with key distribution, and not with authentication. As also explained above, Stallings, insofar as it describes an authentication method, teaches away from the claimed method of authentication. Because Marvit and Burrows are entirely unconcerned with any matter touching upon authentication, neither of those references provides any motivation to change the basic thrust of Stallings which, as explained above, leads away from the claimed invention.

d. Conclusion

On the grounds laid out above, it is respectfully submitted that claim 30 of the present application is patentable over the combination of Marvit, Burrows, and Stallings under the standard of 35 USC §103(a).

VIII. EVIDENCE AND RELATED APPEALS APPENDICES:

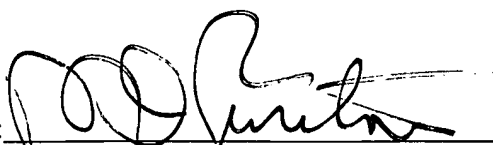
As there are no related appeals and interferences, copies of decisions rendered by a court or the Board for such proceedings do not exist and have not been supplied in an Appendix pursuant to 41.37(c)(1)(x).

As no evidence was submitted and relied upon in this Appeal, an Appendix pursuant to 41.37(c)(1)(ix) has not been supplied.

IX. CONCLUSION

Appellant respectfully requests the Board to reverse the Examiner's obviousness rejection of claims 29-30.

Respectfully submitted,

By: 
Martin I. Finston
Attorney for Appellants
Reg. No. 31,613

Attachment: Appendix X

Date: July 7, 2006

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawford's Corner Road
Holmdel, NJ 07733-3030

X. CLAIMS APPENDIX

1-28 (canceled)

29. A method for authenticating a mobile station to a network B, comprising:

from the mobile station, wirelessly communicating to network B an identifier for the mobile station;

via wireless communications between the mobile station and with a base station A belonging to a network A, transacting with network A to obtain an encryption key K known only to network A and to the mobile station;

via wireless communications with base station A which are secured by key K, obtaining at the mobile station an authentication key SSD known only to network A, to the mobile station, and to a further network B;

via wireless communications with base station A, sending an authentication message from the mobile station to network A to be forwarded to network B, the authentication message comprising the identifier of the mobile station encrypted with SSD; and

if the authentication message is accepted by network B, entering the mobile station into wireless communications with a base station of network B.

30. A method for authenticating a mobile terminal to a network, comprising:

via wireless communications between a mobile station and a network A, transacting with the mobile station to provide it with an encryption key K known only to network A and to the mobile station;

receiving an authentication key SSD and an identifier of the mobile station from a further network B as a result of a request sent from the mobile station to network B, said

request including said identifier, and providing SSD to the mobile station via wireless communications which are secured by key K;

receiving from the mobile station, via wireless communications, an authentication message which comprises said identifier encrypted with SSD; and

forwarding the authentication message to network B.